Guidelines and Resources for Internet Safety in Schools

South Carolina Department of Education
Office of Career and Technology Education

SOUTH CAROLINA
STATE DEPARTMENT
OF EDUCATION

Division of Accountability

Office of Career and Technology Education Associates

Nancy Allen	**Health Science Education**	**nallen@ed.sc.gov**
Dr. Ray Davis	**Career Guidance**	**rbdavis@ed.sc.gov**
Tony Dillon	**Business, Marketing, Finance, and Information Technology**	**tdillon@ed.sc.gov**
Susan Flanagan	**Finance**	**sflanaga@ed.sc.gov**
Pat Flora	**State Plan**	**pflora@ed.sc.gov**
Eleanor Glover	**Family and Consumer Sciences**	**eglover@ed.sc.gov**
Patrice Green	**Civil Rights, Nontraditional, and Special Populations**	**pgreen@ed.sc.gov**
Shawn Larrymore	**Data Collection and Reporting**	**smlarrym@ed.sc.gov**
Merri Long	**Local Plans**	**mlong@ed.sc.gov**
B. T. Martin	**Science, Technology, Engineering and Mathematics (STEM)**	**btmartin@ed.sc.gov**
Amy McCaskill	**CATE Curriculum and Standards**	**amccaski@ed.sc.gov**
Wofford O'Sullivan	***CTCTW*, Professional Development, and Work-Based Learning/Extended Learning Opportunities**	**wosulliv@ed.sc.gov**
Jim Spencer	**Manufacturing**	**jspencer@ed.sc.gov**
Tina White	***Making Middle Grades Work (MMGW)* and *High Schools That Work (HSTW)***	**tlwhite@ed.sc.gov**
Glenda Whittle	**Data Collection and Reporting**	**gwhittle@ed.sc.gov**

Foreword

Today's students will be the first generation to use the Internet for their entire lives. This unprecedented access to resources will enhance their learning, research, communications, explorations for new ideas, and expressions of creativity. Unfortunately, this remarkable resource has become susceptible to abuse that often targets young people.

The South Carolina Department of Education is committed to helping school districts develop and implement Internet safety policies and programs. This document, *Guidelines and Resources for Internet Safety in Schools*, provides a starting point as districts add required Internet safety components to their acceptable use policies. While the document offers recommendations, specific curricular details are left to the discretion of school systems.

The guidelines represents the knowledge and perspectives of educators; researchers; law enforcement officials; local, state, and federal representatives; and independent nonprofit organizations.

As educators, perhaps our greatest priority is to protect the students. In terms of online safety, the ever changing nature of the Internet makes this objective a constantly moving target. Although the task is daunting, we must stay ahead of the curve in detecting and reporting Internet threats and predators. Instructors need to be well informed about the latest computer threats and integrate safety into their curricula throughout the school year. Administrators should keep staff and community members apprised of new developments. They also need to evaluate the Internet safety program's quality and effectiveness and make regular adjustments and revisions.

The Internet's potential is limitless and still largely untapped. Within the next 10 years, it will change education in ways we never could have imagined. My goal is for the state of South Carolina to remain a national leader in educational technology by pioneering cutting edge uses of the Internet while ensuring the safety of each student.

Introduction

Few would argue that the Internet has had a profound influence on education, including an unprecedented access to resources, opportunities for collaboration across geographic and temporal barriers, and engagement in global communities. Current research suggests this impact may extend to student academic achievement. In a recent study of low income students, Linda Jackson and her colleagues at Michigan State University found that increased Internet use correlates with higher standardized reading achievement scores and grade point averages.[1]

High speed Internet has made the Web much more interactive, with communication possibilities expanded beyond the written word. While young people tend to adopt new technologies more quickly than adults, many do not have the experience or knowledge to understand the potential risks. Parents, educators, and community members must encourage students to take advantage of the Internet's benefits while reducing its risks.

All South Carolina school districts currently have Internet acceptable use policies and employ filtering software. These policies and filters are necessary but cannot prevent all risks to students. Since Internet threats change constantly, schools and divisions must take additional steps to safeguard students.

The South Carolina Department of Education has published *Guidelines and Resources for Internet Safety in Schools* to assist school districts in three areas: (1) writing an Internet safety component as part of the acceptable use policy, (2) integrating Internet safety into the curriculum, and (3) fostering responsibility among all stakeholders to help protect young people from online dangers. This document also will explain the meanings of new terms commonly used in cyberspace. Words italicized in the text are explained in more detail in the glossary.

[1] L.A. Jackson, A. von Eye, F.A. Biocca, G. Barbatsis, Y. Zhao, and H.E. Fitzgerald, "Does home Internet use influence the academic performance of low income children?" *Developmental Psychology*, 42(3):17 (2006).

Issues School Districts Must Address

Although the various Internet safety programs across the state will share some common elements, each school district should examine its resources and requirements closely and fashion an appropriate plan that includes the following:

- integration of Internet safety into the curriculum and instruction;

- defined roles and responsibilities for the school board; administrators (central office and building); teachers; counselors; instructional technology resource teachers; library media specialists; building resource officers; technology coordinators; students; and community stakeholders, including but not limited to parents, caregivers, public library staff, afterschool and off campus program instructors, and local law enforcement officials;

- safety measures, including any that already exist;

- data and network security plan;

- procedures to address breaches of Internet security and protect students' safety;

- process for annually reviewing, evaluating, and revising the program;

- professional development opportunities for staff across the school district; and

- outreach programs for community stakeholders;

In revising acceptable use policies, divisions will confront three major issues regarding appropriate and effective Internet use: safety, security, and ethics. Since the existing policies already address Internet ethics, the guidelines in this document focus primarily on safety and security topics.

- **The Internet is a valuable tool**. Like any other tool, the Internet can be misused or dangerous in certain circumstances. Students must learn how to use the Internet safely and effectively.

- **Personal safety on the Internet**. Students must understand that people are not always who they say they are. They should never give out personal information without an adult's permission, especially if it conveys where they can be found at a particular time. They should understand that predators are always present on the Internet. Students should recognize the various forms of *cyberbullying* and know what steps to take if confronted with that behavior.

- **Information on the Internet**. Students and their families should discuss how to identify acceptable sites to visit and what to do if an inappropriate site is accessed. Students should be informed about various Web advertising techniques and realize that not all sites provide truthful information.

- **Activities on the Internet**. Likewise, students and their families should discuss acceptable social networking and communication methods and the appropriate steps to take when encountering a problem. Students should know the potential dangers of emailing, gaming, downloading files, and peer to peer computing (e.g., viruses, legal issues, harassment, sexual predators, and identity theft).

A frequently overlooked element is school and community support for the acceptable use policy. All stakeholders-district staff and community members–need accurate, up to date facts.

In addition, all school personnel should keep abreast of constantly changing Internet safety information and communicate regularly on the topic. Some Internet threats, such as bullies and sexual predators, exist in the community, as well. As a result, administrators, counselors, and resource officers previously have confronted some of the problems now emerging on the Internet.

While devising the revised policy, remember that students may not recognize virtual life safety issues as readily as they might recognize real life safety issues. Virtual life risks often are invisible, unsolicited, and instant. School districts should educate students to recognize potential illegal activities and outline a clear process for reporting problems.

What Students Need To Know

The Internet is a powerful tool that should be used wisely.

- The Internet allows students access to a vast library of previously unavailable.
  Clicky's Web World: What 2 Do on the Web (NetSmartzKids)
  http://www.netsmartzkids.org/activities

- The Internet enables students to communicate with people **(SafeTeens)** around the world. http://www.safeteens.com/

- The Internet provides a creative outlet for students skilled in writing, art, music, science, mathematics, and other topics.

Students need to know that not all Internet information is valid or appropriate.

- Sexually explicit material or violent images can affect students negatively.

- Sexual predators will try to convince students to trust them.

- Internet information may promote negative attitudes, such as hate or intolerance, and dangerous or illegal activities, such as self injuring behavior, gambling, and illegal drug use.

Students should be taught specifically how to maximize the Internet's potential while protecting themselves from potential abuse.

- The critical thinking skills students learn in the classroom, library, and lab should be applied to Internet resources and Web searching.

- Students need to know what to do and who to ask for help when they encounter a person or site on the Internet that is offensive or threatening to them.

- Students and adults are strongly encouraged to be responsible citizens. Report illegal Internet communications and activities to Internet Service Providers and local law enforcement authorities.

Get Your Web License (PBS KIDS) http://pbskids.org/license/

Internet messages and the people who send them are not always what or who they seem.

- People in *chat rooms, instant message* "buddies", or those who visit a *blog* may not be who they appear to be. Students should learn to recognize when someone is potentially dangerous. Students need to realize when an Internet encounter may be questionable and how to protect themselves when this occurs.

- Students need to be aware that their electronic messages, even those with known friends, can leave *electronic footprints* that can be misused by others.

Email can cause *malicious code* infection problems for a computer or network. Students should not open email or attachments from unknown sources. Students need to know which information is safe to share with others online, which should never be shared, and why sharing it could put them at risk. Students should never reveal online any information about where they live or attend school.

iKeepSafe Internet Safety Coalition
http://ikeepsafe.org

Don't Believe the Type: Surf Safer (Cybertipline)
http://tcs.cybertipline.com/surfsafer.htm

Predators and cyberbullies anonymously use the Internet to manipulate students. Students must learn to avoid dangerous situations and get adult help.

- Sexual predators deceive students by pretending to be students themselves. They sometimes lure young people into a false sense of security or blind trust and try to alienate them from their families. Students need to learn about these types of psychological ploys and how to get immediate adult help.

- Bullies use Internet tools, such as *instant messaging* and the Web, to harass or spread false rumors about students. Students need to know how to see proper help in these potentially dangerous situations.

- Students need to know that posting information and pictures can allow predators to contact and begin *grooming* them for illegal meetings and actions. Personal photos can be easily misused or altered when posted on the Internet.

Cyberbullies (McGruff)
http://www.mcgruff.org/#/Advice

Internet Super Heroes: Cyberbullying (use pulldown menus at bottom) (Wired Safety)
http://www.internetsuperheroes.org/cyberbullying/index.html

Internet activities, such as playing games and downloading music or video files, can be enjoyable. Students need to know which activities are safe and legal.

- *Gaming* sites can attract sexual predators and/or *cyberbullies*.
- Some games may contain pornographic and/or violent images. Students need to talk to parents about what is acceptable.
- Students need to know how to detect whether a specific file downloaded is legal and/or free of malicious code.

10 Tips for Dealing with Game Cyberbullies and Griefers (Microsoft)
http://www.microsoft.com/protect/family/activities/griefers.mspx

The 411: File Sharing (StaySafe) http://www.staysafe.org

What Parents, Grandparents, and Caregivers Need to Know

The Internet is a valuable learning, communication, and entertainment provider. A child's Internet use should be based on age and the family's needs and values.

- The Internet can help with research and homework. **Online Safety Guide (click on age level tips on left side of screen) (Get Net Wise)** http://kids.getnetwise.org/safetyguide/

- The Internet can facilitate easy communications with family members and friends. Although the Internet can be educational and entertaining, children should spend time offline.

- Appropriate Internet activities for children should be age related. Teenage activities may not be appropriate for a young child.

Parenting Online (Wired Kids)
http://wiredkids.org/resources/documents/pdf/parentingonline.pdf

Parents must understand potential Internet dangers and prepare their children, just as they prepare them for going to the playground or crossing the street.

- The Internet contains inappropriate information for children, such as pornography, hate literature, aggressive advertising, and violent images. http://www.wiredsafety.org

- Internet communication often is anonymous, especially in chat rooms or blogs. A sexual predator may pose as a friend to lure a child away from his or her family's protection. *Cyberbullies* may target a child for harassment.

- Using email or downloading files can lead to *viruses* or hidden *spyware*, which endanger a family's privacy and computer.

- Information provided over the Internet-by children and adults-can be used for *identity theft*.

Online Predators: Help Minimize the Risk
http://www.microsoft.com/protect/family/guidelines/predators.mspx

Parents can provide the best protection for their children and help reinforce the principles learned in the classroom. Families should reach agreements about acceptable Internet activity and content.

- Parents should read about and know how to respond to Internet risks. They can stay informed by signing up for a family Internet safety newsletter and working directly with their school districts.

  The Children's Partnership: The Parents' Guide to the Information Super Highway
  http://www.childrenspartnership.org/AM/Template.cfm?Section=Speeches_and_Pres

- Parents should talk with their children about safe and appropriate Web sites and activities.

  Staysafe.org for Parents
  http://www.staysafeonline.com

- Children should be encouraged to report anything they feel uneasy about. If parents overreact, children will be less likely to confide in them the next time.

- The family should create rules about what children can and cannot do while online. Posting the agreements near the computer will ensure children see them often.

Monitoring is crucial. Parents should know where their children go online, how long they stay there, and the warning signs that something is wrong.

- Parents should place computers in family areas as opposed to bedrooms; however, they need to realize that *instant messaging* devices, cell phones, and *wireless computers* may allow children to get online anywhere.

- When young children first begin going online, parents should work closely with them and talk about Internet safety at an early age.

- Parents should *bookmark* suitable sites and check back regularly to ensure that the contrite of those sites has not changed and that harmful sites have not been bookmarked.

- *Filters* are helpful but not fail proof. Parents need to know about *circumventor sites*, which allow users to get around *filtering* software controls.

- Parents should seek training to learn different methods of *monitoring* their children's Internet use. They continually need to employ up to date techniques and software to track where their children go online.

- Parents should be aware that some sites have age restrictions that children may ignore or not realize.

- Parents should follow where their children go on the Internet just as they would watch them in a large public area. They need to check regularly the *history* and *bookmarks* or *favorites* on all computers in the house.

- Parents should recognize the warning signs of when a child might be in trouble, doing something they should not be doing, or spending too much time on the Internet. They should know how to report a problem to their Internet Service Provider and local law enforcement officials.

- Some Internet activities are not only dangerous but illegal. Parents should be aware of relevant laws.

Cybertipline (National Center for Missing and Exploited Children) http://www.cybertipline.com/

What Teachers, Instructional Technology Resource Teachers, Library Media Specialists, Counselors, and Resource Officers Need to Know

Classroom Internet use can be exciting, rewarding, and challenging. Students' Internet use should be tailored to their ages.

- Teachers should create age-appropriate activities for students.
- Students' varying developmental stages and Internet skills will produce different issues and problems for each age group.
- Educators should maintain open communication with parents about student's academic Internet use-in guided classroom settings and independently.

Monitoring is crucial.

- *Filters* are not fail proof. Teachers and librarians must watch where students go on the Internet-just as they would keep an eye on them during a field trip. Computer labs may be configured to assist with this supervision.
- Students should not be allowed to wander aimlessly on the Internet. Teachers must provide an academic purpose before allowing students to go online.
- Teachers need to acquaint themselves with new tools that allow students to visit protected sites. As much as possible, they should go into *history* and examine the pages students have viewed.
- Classroom and library rules must comply with the districts acceptable use policy regarding the steps students should take after accidently accessing an inappropriate site.

- Technical staff need to utilize the district's network tracking controls and study the generated reports, which may identify patterns of inappropriate use.

  How To (staysafe.org)
  http://www.staysafeonline.com

- Teachers need to keep up to date on Internet safety issues and provide accurate timely information to students.

Student technological interactions in the virtual world can be negative and spill over into the real world.

- Educators need to learn about *cyberbullying*, recognize the signs of a bullied student, and know what to do about it.

- Students must be taught which types of personal information are safe to share with others.

- Online and wireless communications-even with known friends or peers-can compromise students' privacy as technology savvy predators may eavesdrop.

- Students must understand that people are not always who they claim to be and that Internet information is not always accurate or appropriate.

Exchanging information with others is a great way to use the Internet but also possesses inherent dangers.

- Educators must know and enforce school policies on exchanging or downloading files.
- School staff should be alerted continually about potential email dangers and learn how to recognize the problem signs.
- Online journals and *blogs*, even when password protected, may reveal more personal information than a student intends. Technology savvy predators can circumvent many safeguards offered by journal and *blogging* sites.
- Educators should check the age appropriateness of any *social networking* sites that students visit.

Students need to hear the rules often.

- Teachers should establish and post rules for safe Internet use near computers in classrooms, libraries, and labs.
- Students should be reminded regularly that the rules are intended to ensure their safety.
- Teachers should go over the rules with students periodically. As a result, the students-even when excited or upset-will be more likely to remember the rules.
- Students and their parents should know the consequences of disobeying the rules. Educators must keep the lines of communication open with students and parents.
- Schools must be consistent and fair in enforcing classroom rules and the district's acceptable use policy.

  Kids' Rules for Online Safety (SafeKids.com)
  http://www.safekids.com

What School Administrators Need To Know

School administrators should play key roles in developing and implementing a district policy that protects children on the Internet. They ultimately must enforce the district's acceptable use policy and understand the information needs of all stakeholders: teachers, instructional technology resource teachers, technology personnel, library media specialists, counselors, principals, resource officers, parents, local law enforcement agencies, and civic organizations.

Administrators must oversee all aspects of the Internet safety program.

- Review annually the district's technology infrastructure with appropriate technology staff, making improvements as needed.

- Monitor the quality and effectiveness of Internet safety information presented to the respective stakeholder groups.

- Incorporate Internet safety into the district's professional development plans and community outreach programs.

- Schedule continuing professional development to keep educators aware of the most recent Internet safety developments.

The Internet is invaluable, educationally and administratively; however, as with all tools, it can be misused and dangerous. In addition, the Internet constantly changes.

- Administrators should understand the Internet's educational advantages and how it is used throughout the division.

- Administrators must understand the potential risks of using the (1) Internet for instruction and (2) technology networks for data collection, storage, and communication.

- Administrators should stay up to date with new developments in capabilities, vulnerabilities, and legal issues related to the Internet and school responsibilities.

- Schools should appoint a staff member-a security officer or other appropriate person-to make sure this policy is implemented.

As with any system, the district must have clear and effective policies and procedures in place to protect students and help prevent misuse of the system.

- A systematic review of policies and procedures needs to be carried out at least yearly.

- Since risks cannot be completely eliminated, the division should be prepared to handle a crisis.

- *Filters* are helpful but not fail proof. As students become more experienced, they may use *circumventor sites* to get around *filtering* software controls.

- Funding for security and safety technology should be anticipated and planned.

Communication among all stakeholders is imperative for safety and security policies to be effective. Although a school's legal responsibility does not extend to home Internet use, school leaders can help prevent tragic situations by ensuring parents and students are well informed.

- Administrators should inform parents regularly about new Internet safety information.

- Students and parents must know the policies and the consequences associated with violations.

- Professional development on Internet safety must be a high priority.

- Funding needs to be budgeted regularly for better communication and training, which must be evaluated for its effectiveness.

- The acceptable use policy's Internet safety component should clearly emphasize that protecting children is a high priority.

What School Boards Need to Know

Each school board must review and approve its district's revised acceptable use policy and implementation plan as presented by the superintendent. The board must ensure the policy complies with current federal, state, and local laws related to Internet safety.

The Internet is invaluable, educationally and administratively; however, as with all tools, it can be misused and dangerous. In addition, the Internet constantly changes.

- The board should understand the Internet's educational advantages and how it is used in the district.

- The board must understand the potential risks of using the (1) Internet for instruction and (2) technology networks for data collection, storage, and communication.

- Board members should stay up to date with new developments in capabilities, vulnerabilities, and legal issues related to the Internet and school responsibilities.

As with any system, the district must have clear and effective policies and procedures to protect students and prevent misuse. Policies and procedures also must be in place for crisis management.

- A systematic review of policies and procedures need to be carried out at least yearly.

- Since risks cannot be completely eliminated, the district should be prepared to handle a crisis.

- Funding for security and safety technology should be anticipated and planned.

Communication among all stakeholders is imperative for safety and security policies to be effective. Although school legal responsibility may not extend to home Internet use, school staff can help prevent tragic situations by ensuring parents and students are well informed.

- Providing information to parents should be a priority.

- Students and parents must know the policies and the consequences associated with violations.

- Professional development for all educators on Internet safety should be a high priority.

- Funding needs to be budget regularly for better communication and training, which must be evaluated for its effectiveness.

National School Boards Association Technology Page
http://www.nsba.org/SecondaryMenu/TLN.aspx

Education Law Organization
http://www.educationlaw.org/

APPENDIX

Appendix A

Internet Safety and the Standards of Learning for Computer/Technology

Social and Ethical Issues

The student will practice responsible use of technology systems, information, and software.

- Know the school's rules for using computers.
- Understand the importance of protecting personal information or passwords.
- Understand the basic principles of the ownership of ideas.

The student will use technology responsibly.

- Demonstrate respect for the rights of others while using computers.
- Understand the responsible use of equipment and resources.

The student will demonstrate knowledge of ethical, cultural, and societal issues related to technology.

- Identify how technology has changed society in areas such as communications, transportation, and the economy.
- Discuss ethical behaviors when using information and technology.

The student will practice responsible use of technology systems, information, and software.

- Understand the need for the school division's acceptable use policy.
- Discuss the rationale of fair use and copyright regulations.
- Follow rules for personal safety when using the Internet.

The student will demonstrate knowledge of technologies that support collaboration, personal pursuits, and productivity.

- Work collaboratively when using technology.
- Practice and communicate respect for people, equipment, and resources.
- Understand how technology expands opportunities for learning.

The student will demonstrate knowledge of ethical, cultural, and societal issues related to technology.

- Demonstrate knowledge of current changes in information technologies.
- Explain the need for laws and policies to govern technology.
- Explore career opportunities in technology related careers.

The student will practice responsible use of technology systems, information, and software.

- Demonstrate the correct use of fair use and copyright regulations.
- Demonstrate compliance with the school division's Acceptable Use Policy and other legal guidelines.

The student will demonstrate knowledge of technologies that support collaboration, personal pursuits, and productivity.

- Work collaboratively and/or independently when using technology.
- Practice preventative maintenance of equipment, resources, and facilities.

Appendix B

Web Based Resources on Internet Safety

This appendix lists Web sites related to Internet Safety. All web sites were accurate and online as of April 28, 2009.

Age Appropriate Guidelines for Internet Use

Age Based Guidelines for Kids' Internet Use by Microsoft
http://www.microsoft.com/protect/family/age/stages.mspx
- Guide to how children of different ages use the Internet

Be Web Aware by Media Awareness Network (see Safety Tips by Age on left side of screen)
http://www.bewebaware.ca/english/default.aspx
- Safety tips by age (left side menu)

Get Net Wise: Online Safety Guide by Internet Education Foundation
http://kids.getnetwise.org/safetyguide/
- A parent's perspective and information about online privacy

Copyright (see Ethics)

Cyber-bullying

Be Web Aware: Challenging Cyber-Bullying by Media Awareness Network
http://www.bewebaware.ca/english/CyberBullying.aspx
- Legal overview, role of Internet service providers, and taking action

Cyber-bullies by National Crime Prevention Council
http://www.mcgruff.org
- Tips for avoiding and handling cyber-bullies

Cyber-bully home page by Cyberbully.org (Nancy Willard)
http://www.cyberbully.org/
- Very helpful information with several downloadable handouts

Cyber-bullying: Research by Cyberbully.us
http://www.cyberbullying.us/research.php
- Research and other helpful information

Prevent Cyber-bullying & Internet Harassment
http://www.cyberbully411.org/
- Resources for prevention

STOP cyber-bulling by Wired Kids
http://www.stopcyberbullying.org/index2.html
- Legal overview, prevention, and reporting

Stoptextbully.com by NCH
http://www.stoptextbully.com/
- Downloadable posters

Definitions

Be Web Aware: Internet 101 by Media Awareness Network
http://www.bewebaware.ca
- Short glossary of several Internet terms

Glossary by Symantec
http://www.symantec.com/business/security_response/glossary.jsp
- Extensive online glossary

On Guard Online: Glossary by Federal Trade Commission
http://www.onguardonline.gov/tools/learn-terms.aspx
- Standard glossary of computer terms

Email

Be Web Aware: Spam by Media Awareness Network
http://www.bewebaware.ca
- Tips for parents regarding spam

Get Net Wise: Risks by Technology: Email by Internet Education
http://kids.getnetwise.org/safetyguide/technology/email
- Basic overview of spam and junk mail

Help keep spam Out of Your Inbox by Microsoft
http://www.microsoft.com/protect/yourself/email/spam.mspx
- Tips and filters for blocking junk mail

On Guard Online: Spam Scams by Federal Trade Commission
http://www.onguardonline.gov/spam.html
- List of popular scams and recommendations for avoiding problems
- Maintaining student safety and privacy

Ethics

Cyber ethics by U.S. Department of justice, Computer Crime & Intellectual Property Section
http://www.cybercrime.gov/cyberethics.htm
- Links to sites about cybercrime

Respect copyrights.org by Motion Picture Association of America
http://www.respectcopyrights.org/index.html
- Issues involved with illegal downloads

Filtering

Filtering and Blocking by Wired Kids
http://www.wiredkids.org/safesites/filtering.html
- Information about filtering, blocking, and outgoing software

Filter Review.com by National coalition for the Protection of Children and Families
http://www.filterreview.com
- Background for selecting the most appropriate filters

The X Lab: Internet Safety for Children by The X Lab
http://www.thexlab.com/faqs/internetsafetychild.html
- Listing of filtering software for Macs

Hate Sites

Be Web Aware: Violent and Hateful Content by Media Awareness
http://www.bewebaware.ca
- Information about violent content, online hate, and what parents should do

Hate on the Internet: A Response Guide for Educators and Families by Partners Against Hate
http://www.partnersagainsthate.org/publications/hoi_full.pdf
- Advice and tools for helping students manage exposure to hate sites
- An overview of hate sites, laws, and how to help students deconstruct them

How the Internet Works

How Does the Internet Work? By U & I Learning (commercial site – no advertising)
http://hwi.uni.be/archief/en/index.htm
- Animated modules that explain how the Internet works

The Internet Tutorial by Dynamic Web Solutions (commercial site – no advertising)
http://www.dynamicwebs.com.au/tutorials/history.htm
- Tutorials that explain the workings of the Internet

Identity Theft

Fighting Back against Identity Theft by Federal Trade Commission
http://www.ftc.gov/bcp/edu/microsites/idtheft/

- Resources about identity theft, including a printable brochure and PowerPoint slides

OnGuard Online: ID Theft by Federal Trade Commission
http://www.onguardonline.gov/topics/identity-theft.aspx

- Steps to take in case of identity theft

Recognize Phishing Scams and Fraudulent Emails by Microsoft
http://www.microsoft.com/protect/yourself/phishing/identify.mspx

- Basic overview of phishing scams

Instant Messaging

10 Tips for Safer Instant Messaging by Microsoft
http://www.microsoft.com/protect/yourself/email/imsafety.mspx

- Suggestions for using instant messaging

International, National, and State Organizations

ChildNet International home page
http://www.childnet-int.org/

Cyberbullying.org home page
http://www.cyberbullying.org/

Get Net Wise home page by Internet Education Foundation
http://www.getnetwise.com/

Internet Safety by Polly Klaas Foundation
http://www.pollyklaas.org/internetsafety/index.html

iSAFE homepage by Internet Safety Foundation
http://www.isafe.org/

Kidz Privacy by Federal Trade Commission
http://www.ftc.gov/bcp

National Center for Missing and Exploited Kids home page
http://www.missingkids.com/

Net Smartz Workshop by National Center for Missing & Exploited Kids
http://www.netsmartz.org/

ProtectKids.com home page by Enough is Enough
http://www.protectkids.com

SafeKids.com home page
http://www.safekids.com

Web Wise Kids home page by Web Wise Kids
http://www.webwisekids.org/

WiredSafety.org home page by Wired Kids (includes Teen angels, Wired Safety, and Wired Kids)
http://www.wiredsafety.org/

Internet Benefits and Risks

Cybercrime by National Association of Attorneys General
http://naag.org/publications_cybercrime.php
- Online articles about different aspects of cybercrime

Parenting Online by Wired Kids
http://wiredkids.org/parents/parentingonline/index.html
http://wiredkids.org/resources/documents/pdf/parentingonline.pdf (printable version)

What Are The Risks by SafeKids.com
http://www.safekids.com
- Brief overview of potential risks

Legal: National

Education Law Association home page
http://www.educationlaw.org
- Developed by educational and legal scholars

Internet Safety Policies and CIPA: An E-Rate Primer for Schools and Libraries by E-Rate Central
http://www.eratecentral.com/CIPA/cipa_policy_primer.pdf

- Requirements for federal funding related to the Children's Internet Protection Act (CIPA)
- Neighborhood Children's Internet Protection Act (NCIPA)

School Law in Review 2006 by National School Boards Association
http://secure.nsba.org/pubs/item_info.cfm?ID=727

- CDROM, available for purchase, including most aspects of education law

School Law: Technology by National School Boards Association
http://www.nsba.org/site/page.asp?TRACKID=&CID=397&DID=8638

- Legal technology information, including resources, news, and recent cases

Newsletters, Blogs and Podcasts

Get Net Wise News by Get Net Wise
http://www.getnetwise.com

Internet Safety – For Our Children's Sake by Jace Shoemaker Galloway
http://internetsafetyadvisor.squarespace.com/journal/

- Internet safety blog maintained by a Midwestern school leader

iSAFE Times, iEDUCATOR Times, and iPARENT Times by iSAFE
http://www.isafe.org/channels/sub.php?ch-op&sub_id=4

NetsSmartz Bulletin by National Center for Missing & Exploited Children and Boys & Girls Clubs of America
http://www.netsmartz.org/feedback/bulletin.htm

OnGuard Online: USCERT Alerts by Federal Trade Commission
http://onguardonline.gov/certalerts.html

SafeKids.com home page
http://safekids.com/

- "Timely articles" link features up to date information

Online Games

Parent/Child Sample Agreements

Family Contract for Online Safety by SafeKids.com
http://www.safekids.com/contract.htm
- Kid's Pledge and Parent's Pledge
- Clear List of commitments

Kids' Rules for Online Safety by SafeKids.com
http://www.safekids.com/kidsrules.htm

Rules 'N Tools Youth Pledge by ProtectKids.com
http://www.protectkids.com/parentsafety/pledge.htm
- Family Internet Safety contract

Peer to Peer (P2P) or File Sharing

On Guard Online: P2P File Sharing by Federal Trade Commission
http://onguardonline.gov/p2p.html

Professional Development

Every K12 Professional's Guide to the New Literacies Associated with Information and Communication (ICT) and Higher Student Achievement by Cyber Smart!
http://www.cybersmart.org/pd/
- Free online course for groups of 25 or more
- Free training with online video modules and lesson plans; requires login id

Reporting Problems

Cyber Tipline by National Center for Missing & Exploited Children
http://www.cybertipline.com/
- Reporting mechanism for child sexual exploitation

Get Net Wise: Reporting Trouble by Internet Education Foundation
http://kids.getnetwise.org/trouble/
- Identifying, reporting, and educating children about online crimes

Appendix C

Glossary

Blog/blogging: This term is derived from Web log and is an increasingly popular type of web site. Most take the form of journal entries and allow readers to post comments.

Bookmark(s): This browser features stores a Web address in memory and allows the user to link quickly to the site.

Chat rooms: These Web Sites or online services facilitate electronic discussions by quickly posting the comments and responses of multiple users.

Circumventor sites: These parallel Web sites allow children to get around some filtering software and access sites that have been blocked.

Cyberbullies/cyberbullying: This refers to any online threats by one student toward another, typically through emails or on Web sites (e.g., blogs, social networking sites.)

Cybercrime: This refers to any Internet related illegal activity.

Cybersecurity (sometimes cyber security): This refers to any technique, software, etc., used to protect computers and prevent online crime.

Cyberstalking: This refers to a number of methods individuals use to track, lure, or harass another person online.

Electronic footprints: Computers maintain a record of all Web sites visits and email messages, leaving a trail of the user's activity in cyberspace. These data can still exist even after the browser history has been cleared and email messages have been deleted.

Favorite(s): This is the name for bookmarks (see above) used by Microsoft's Internet Explorer browser.

File sharing: This software enables multiple users to access the same computer file simultaneously. File sharing sometimes is used illegally to download music or software.

Filter/filtering: This refers to different types of software that screen and block online content.

Gaming: This term describes Internet games, which can be played either individually or by multiple online users at the same time.

Griefers: These internet users intentionally cause problems for other gamers.

Grooming: This refers to the techniques sexual predators use to get to know their victims in preparation for sexual abuse.

History: This is a tracking feature of Internet browsers that shows all the recent Web sites visited.

Identify theft: In this crime, someone obtains the vital information (e.g., credit card, Social Security, bank account numbers) of another person, usually to steal money. Email scams, spyware, and viruses are among the most typical methods for stealing someone's identity.

Instant messages/messaging: Known by the acronym IM, this is a variation of chat rooms that allows users to communicate through text messages.

Malicious code: This refers to any computer code that is intentionally introduced into a system to damage or destroy files or disrupt the operation of a computer.

Monitoring: this refers generally to the technique of tracking where people have been on the Internet by looking at the history of the browser. It also refers to software used for the same purpose.

P2P (see peer to peer computing)

Peer to peer (P2P) computing: This is a popular way for Internet users to share one another's computer files – usually music, game, or software files.

Phishing: This scam involves sending a fraudulent email soliciting credit card, Social Security, or other personal information from an unsuspecting user.

Social networking: This refers broadly to online communities where people share information about themselves, music files, photos, etc. There are many social networking sites (e.g., MySpace, Facebook, or Twitter).

Spam: This refers to any unsolicited email, or junk mail. Most spam is either a money scam or sexual in nature. Internet Service providers, email software, and other software can help block some, but not all, spam.

Spyware: This refers to a wide variety of software installed on people's computers without their knowledge. The programs typically will track computer use and create numerous popup ads. In some instances, the spyware can damage the computer and facilitate identify theft.

Viruses: These are software programs that typically arrive through email attachments and multiply on the hard drive, quickly exhausting the computer's memory. A Trojan is a variation that allows multiple unauthorized users access to the computer, from which they can send infected emails or spam.

Wireless computers: Many networks now allow computers access to the Internet without being connected with wires. These networks are becoming increasingly more popular and powerful, allowing people to access the Internet using cell phones and other devices.